Privacy and Security Solutions for Interoperable Health Information Exchange

Interim Assessment of Variations Report

Subcontract No. 8-321-0209825

RTI Project No. 9825

Prepared by:

Dana Ashley Green, CPA; Kelly Coyle, J.D.; Diedra Garlock
Michigan Public Health Institute
Okemos, Michigan

Submitted to:

Linda Dimitropoulos, Project Director
Privacy and Security Solutions for
Interoperable Health Information Exchange

Research Triangle Institute
P. O. Box 12194
3040 Cornwallis Road
Research Triangle Park, NC 27709-2194

Date: November 6, 2006

RTI INTERNATIONAL

Table of Contents

Executive Summary

Michigan's HISPC Assessment of Variation effort as executed was a high-touch, hands-on effort to obtain a wide variety of responses and stakeholder representation. Volunteer stakeholders were enthusiastic, candid and well prepared. A significant number of volunteers requested inclusion in subsequent phases of the project. Individual meetings were conducted with the following stakeholders:

HCAM (Nursing Facilities)

MAFP (Family Physicians)

MPCA (Primary Care)

Mid-size, Non Profit Employer(Human Resources)

Michigan Department of Community Health (MDCH) Public Health

Central Michigan Small to Medium Sized Hospital (Rural Health)

Western Michigan Large, Multi-Facility Hospital (Urban Health)

MALSAO (Substance Abuse)

Upper Peninsula RHIO (Indian, Rural)

MALPH (Local Public Health)

Southeastern Michigan Hospital & Emerging RHIO (Urban/Inner Health & RHIO)

MHA (Hospital Association)

MPA (Rx)

Michigan State Police

MHHA (Home Health)

Central Michigan Hospital-based Pharmacy (Rx)

MDCH (Bioterrorism)

Large, Union-related Employer

County Department of Health (Public Health)

Eastern Michigan Small Sized Hospital (Indian, Rural)

Large, Regional, University-based Health system

We were unable to schedule the largest, non-governmental payer in Michigan prior to the report deadline, but will meet with them before the end of November, and include their input in the final report.

Details of our findings are included in the scenario summaries below, and where appropriate, we have included citations to pertinent state law as appropriate. The diversity of responses are evident in the details below.

1. Methodology Section

Original Approach (Scenario Centric) –

1. Set up conference call dates.
2. Created eFlyers describing the project, soliciting participation & listing all the call dates.
3. Emailed the flyers to all health related professional organizations in Michigan.
4. Conducted the conference calls.

Result: Virtually no participation.

Plan B (Expertise Centric) –

1. Analyzed the matrix of scenarios vs. stakeholders to determine exactly with whom we needed to meet.
2. Prioritized the list to fit within the time frame available, (roughly 7 weeks.)
3. Hired marketing consultant with over 10 years experience in healthcare information dissemination in Michigan to manage the meeting logistics. They:
    a. Created a telephone script that was informative and persuasive.
    b. Matched the professional organizations to our wish list.
    c. Contacted professionals and obtained volunteer participation.
    d. Contacted volunteer & arranged appointments then emailed confirmation of the appointments, a summary project flyer, a preparation guide to focus the volunteer's expertise as it related to the scenarios, and copies of the scenarios.
    e. Obtained detailed location and access information to each interview site.
4. Conducted the interviews
5. Summarized the results in the workbook.
6. Emailed the workbook and the scenarios to all volunteers for review.

Result: We are very pleased with the results of our efforts. We believe we have a good cross section of stakeholder input, the candor was excellent and the participants were universally enthusiastic about the project and the process. All volunteers were extremely prepared and some went beyond our most optimistic expectations. We plan to augment our work as needed for the final report.

2. Summary of Relevant Findings Purposes for Information Exchange

2.1 Treatment (Scenarios 1–4)

2.1.1 Stakeholders

Stakeholders for these four scenarios included: Hospitals, clinicians, physician groups, federal health facilities, community clinics and health centers, long term care facilities and nursing homes, and correctional facilities.

2.1.2 Domains

1. User and entity authentication

- Director of Nursing authenticates Dr. X & issues temporary access to EHR
- User IDs & Passwords are assigned to individual users to the system
- Provider electronically signs document

2. Information authorization and access controls

- Obtain a BA with all outside services that use PHI (e.g. Transcription service)
- Terminate temporary access to EHR
- Full provider credentialing is required to gain access to patient EHR
- Provider would need to sign a confidentiality agreement in order to gain access to the system
- Patient signs an Authorization, or release of data authorization language is included in the NPP
- If the patient is incoherent, have daughter sign release
- If the patient is coherent, have patient sign release.
- Access allowed for only those providers who are affiliated with patient's case, through pre-existing order or because the patient has been admitted by a

provider, (in nursing home, a provider has to be responsible for the patient's care.)

- Staff would require a request on letterhead be faxed in and a followup phone call to determine the legitimacy of the access request.

3. Patient and Provider identification

- A central database of credential providers is maintained. Facilities, provider groups and payers all agree to the base standards and share this information rather than credentialing independently. Providers are re-credentialed every 3 years and sanctions are monitored on a continual basis. Virtually all providers are included in every facility roster as a result.

4. Information transmission or security or exchange protocols

- Trading Partners agree to use the same data coding standards so shared data can be interpreted.
- Make copies of pertinent parts of medical records and Mail or fax to trading partner
- Provider would need to print out a hard copy of his notes to be re-entered into the hospital's EHR
- Patient hand carries, provider faxes or mails PHI
- Access from one entity to another is provided via a secure connection or VPN
- PHI is encrypted prior to transmission. The encryption key is sent separately
- A copy of PHI is burned to a CD and patient hand carries or the CD is mailed to other facility

5. Information protection (against improper modification)

- Provide read-only access to ePHI

6. Information audits that record and monitor activity

- All user activity is logged and audit logs are reviewed on a regular basis. Penalty for improper access, use or disclosure includes terminated access for life, termination of employment or suspension.

- A complete list of users who have accessed the EHR is displayed each time anyone access a patient record.

7. Administrative or physical security safeguards

- MH ward is locked with key card or authenticated access. Reception is responsible for authenticating providers before allowing access.

- Transfer paper files via the Walleroo

- Information is zip, encrypted & password protected & emailed. The password and encryption key is emailed separately, or provided via a phone call.

8. State law restrictions

- Complete DCH form 3877 Preadmission Screening for Mental Illness/Developmental Disability Identification for Level 1 screen. If a level 2 screen is suggested, either complete a form DCH 3878 Mental Illness/Developmental Disability Exemption Criteria Certification, or a Level 2 screen.

- Would assume genetic test results of deceased relatives unattainable

- MH, SA & HIV/Aids info is segregated from other patient data is only accessible to provider, PA or NP assigned to case. Release is restricted to express consent.

9. Information use and disclosure policy

- Only allow Dr. X access to relevant information

- Medical records of deceased patients can be obtained via a Letter of Authority

2.1.3 Critical Observations

Credentialing prior to allowing access is a goal of many of the stakeholders. However the overriding barrier with credentialing is the time issue. It can take up to several weeks to get credentialing data into a system. Clearly this is not able to be completed in a timely manner. In addition, only allowing credentialed providers to have access, begs the question of how to handle temporary users who are not credentialed but who need immediate access. Other stakeholders looked to see if providers were affiliated with a patient before granting access, and still others used back end logging to ensure that only those with a need to know had access.

Barriers identified also included the need for providers to print out a hard copy of their notes to be re-entered into a hospital's HER and the lack of clarity of stakeholders on the process of obtaining access to genetic test results of deceased relatives of a patient.

2.2 Payment (Scenario 5)

2.2.1 Stakeholders

Stakeholders for this scenario included: Hospitals

2.2.2 Domains

1. User and entity authentication

- User IDs & Passwords are assigned to individual users to the system

2. Information authorization and access controls

- Would require a letter on company letterhead from known contact at payer organization requesting access for a (short) list of users. List would need to be approved by Security officer and related director before user ids & passwords were issued
- Full access to EHRs would require the system to have the capability to restrict access to only those patients covered by that carrier
- Patient signs an Authorization or release of data authorization language is included in the NPP
- Guest users would need to attend training on use of system and Policies and procedures
- User IDs are terminated when an employee quits and all user ids are reviewed on a regular basis to determine if they should be still active.
- Access request would be reviewed and approved by Privacy Officer prior to issuing user ids & passwords
- Only provide PHI to payers by request and after determination that the information is needed for payment
- Full access is granted to case manager based on insurance coverage

3. Patient and provider identification

- A central database of credential providers is maintained. Facilities, provider groups and payers all agree to the base standards and share this information rather than credentialing independently. Providers are re-credentialed every three years and sanctions are monitored on a continual basis. Virtually all providers are included in every facility roster as a result.
- A central database of authorized users is maintained by each entity in a central web-based facility. Facilities, provider groups and payers all agree to the base standards and share this information.

4. Information transmission security or exchange protocols

- Access from one entity to another is provided via a secure connection or VPN

5. Information protection (against improper modification)

- Guest users would have to assure that the computers used to access system have current anti-virus software; in a secure site and that they will abide by HIPAA standards.

- Provide read-only access to ePHI

6. Information audits that record and monitor activity

- All user activity is logged and audit logs are reviewed on a regular basis. Penalty for improper access, use or disclosure includes terminated access for life, termination of employment or suspension.

- A complete list of users who have accessed the EHR is displayed each time anyone access a patient record.

9. Information use and disclosure policy

- Only allow access to relevant information

- Conduct conference calls to discuss and share encounter information.

- Obtain separate authorization from patient for this use/disclosure

- Provider & staff review disclosure request so that only the minimum necessary information is disclosed

- Provider & staff review disclosure request so that only the minimum necessary information is disclosed

- No access granted to Insurance companies.

2.2.3 Critical Observations

For the payment scenarios, granting access for those who need temporary or immediate use in a timely and HIPAA compliant manner is a prevailing issue.. A notable barrier that was identified: one stakeholder's policy of placing a lifetime ban on any individual who inappropriately accesses medical records.

2.3 RHIO (Scenario 6)

2.3.1 Stakeholders

Stakeholders for this scenario included: Clinicians, physician groups, professional associations and societies, pharmacies, homecare, and hospice

2.3.2 Domains

1. User and entity authentication

- User IDs & Passwords are assigned to individual users to the system

2. Information authorization and access controls

- Patient signs an Authorization, or release of data authorization language is included in the NPP that the patient signs
- Participation by providers would have to be voluntary

9. Information use and disclosure policy

- Unless there is some compelling reason, data used for quality measures are limited to de-identified data
- Providers don't want competition to see their rank. Would participate if and only if they received useful information and the information was limited by practice
- NPP includes an option for the Patient to Opt-Out of the use/disclosure
- Providers must also have the authorization to be granted access to the data to use for non-clinical purposes.
- Do not consider this a appropriate use of a RHIO agreement

- Patient would have to sign a consent to opt-in to the study
- In order to gain full picture, would need Pharmacist data, OTC, PBM and Mail order information. Very few RHIOs have complete Rx participation
- Would provide full access to Rx data for quality study
- A business associate agreement with RHIO would be required
- Providers would want full de-identified dataset to study nuances of the data that might explain variances

2.3.3 Critical Observations

Emerging RHIOS in Michigan are in need of consistent federal and state guidance and standardization. Different (and generally conservative) interpretations of HIPAA, federal and state laws create barriers for health information exchange. Quite frankly, providers are also fearful of being monitored and reported on based on performance data collected from RHIOs.

Providers are currently unwilling to sanction the non-clinical use of RHIO data.

And perhaps one of the biggest barriers for RHIOs is establishing trust between the organizations that will exchange sensitive information.

2.4. Research (Scenario 7)

2.4.1 Stakeholders

Stakeholders for this scenario included: Medical and public health schools that undertake research

2.4.2 Domains

1. User and entity authentication

- User IDs & Passwords are assigned to individual users to the system

2. Information authorization and access controls

- Separate parental consent to participate in research is required for 13 year olds. There are separate age cohort restrictions, the process is currently manual
- Patient signs an Authorization or release of data authorization language is included in the NPP

4. Information transmission security or exchange protocols

- PHI is encrypted prior to transmission. The encryption key is sent separately
- State would require a Data Use agreement before releasing data for research purposes

5. Information protection (against improper modification)

- Any changes to approved protocol require an amendment to the IRB protocol and a new review by the IRB board

7. Administrative or physical security safeguards

- PHI is kept on a segregated, secure network drive
- Any adverse event, including a breach must be reported to the IRB and reviewed by the IRB. The IRB has a number of options for response -- including shutting down the project
- Data Use agreements are only valid for one year & must be renewed prior to the expiration or the project must be shut down
- If demographic information is needed for the research, it is held separate from the clinical data & only joined on an as needed basis, in a secure environment. Access is limited to only select users

8. State law restrictions

- Any changes to approved protocol require an a new consent form from both subjects and parents

9. Information use and disclosure policy

- Any changes to approved protocol require an amendment to the IRB protocol and a new review by the IRB board
- Unless there is some compelling reason, data used for research would be limited to de-identified data
- Any changes to approved protocol require an a new consent form from both subjects and parents.

2.4.3 Critical Observations

This scenario brings attention to an Institutional Review Board's authority to delay and shut down projects that fail to comply with protocols, obviously this might be considered a barrier, but not in the clinical sense. Most research projects are not critical to front end clinical care and generally, IRB's protect participant's privacy. In addition, not one, but two separate authorizations from the subject to use data are required, and a third if the subject is a minor.

2.5 Law Enforcement (Scenario 8)

2.5.1 Stakeholders

Stakeholders for this scenario included: State Police and Hospitals.

2.5.2 Domains

1. User and entity authentication

- Access to systems are controlled through the use of user ids and passwords.
- User IDs & Passwords are assigned to individual users to the system.

2. Information authorization and access controls

- User IDs are terminated when an employee quits and all user ids are reviewed on a regular basis to determine if they should be still active.
- Initially, the officer would request from the patient authorization to use the State Police standard blood draw (by a medical provider). If patient agrees, the hospital staff will use the State Police blood draw.

4. Information transmission security or exchange protocols

- Access from one entity to another is provided via a secure connection or VPN
- The Law Enforcement Network is double fire walled.
- Provider makes copies of pertinent parts of medical records and Mail or fax to trading partner
- Lab results would be dictated and copied into medical record.

6. Information audits that record and monitor activity

- All user activity is logged and audit logs are reviewed on a regular basis. Penalty for improper access, use or disclosure includes terminated access for life, termination of employment or suspension.

7. Administrative or physical security safeguards

- Case would be tracked in the Law Enforcement Network, a secure portal operated by the State Police.

9. Information use and disclosure policy

- Relatives of Adults have no rights to access PHI -- patient must sign release to give them access.

- If patient refuses to allow State blood draw, officer will obtain a search warrant to compel compliance.

- If the patient will not allow access to the medical record, the officer can obtain a subpoena to acquire the information.

2.5.3 Critical Observations

While no barriers were noted, the process can be labor intensive. This scenario also highlighted the dramatically different procedures law enforcement officials and medical personnel handle similar situations.

2.6 Prescription Drug Use/Benefit (Scenarios 9 and 10)

2.6.1 Stakeholders

Stakeholders for this scenario included: Clinicians, Physician groups, Pharmacies, Hospitals, and Professional associations and societies

2.6.2 Domains

2. Information authorization and access controls

- PBM would need to sign a confidentiality agreement in order to gain access to the de-identified data.

- Would call back phone number for new user to authenticate user.

- Since prescription is for MH diagnosis, the chart would be flagged as restricted

4. Information transmission security or exchange protocols

- Dr. would ask for a copy of a blank PA from PBM, complete the form & fax it back.

9. Information use and disclosure policy

- As part of the patient signing up for the Rx benefit, language is included that allows the PBM to obtain information necessary to determine coverage for non-formulary prescriptions.
- Provider & staff review disclosure request so that only the minimum necessary information is disclosed.
- No access to EHR granted to Insurance companies.
- User IDs & Passwords are assigned to individual users to the system.
- Trading Partner/Business Associate agreement needs to exist between PBM and pharmacy.
- PBM2 would not cooperate with PBM1.
- PBM1 could obtain a de-identified dataset from the company, price it & the company could compare to the price charged by PBM2

2.6.3 Critical Observations

These two scenarios highlight the lack of trust between competitors (PBM1 & PBM2) and between providers and payers. While a limited number of hospitals would allow a payer full access to their patient records, the majority either did not have the technical ability to limit access by payer, or did not see the need to open their systems to a payer.

Another pertinent discussion arose on the lack of critical information between pharmacists, providers and PBMs. Providers are not notified when a prescription they have written is filled; pharmacists and PBMs do not receive a diagnosis, and without joining information held independently by PBMs and pharmacists, a complete drug profile is impossible. Drug related errors could be reduced dramatically if this critical information were routinely shared.

2.7 Healthcare Operations/Marketing (Scenarios 11 and 12)

2.7.1 Stakeholders

Stakeholders for this scenario included: Hospitals and professional associations and societies.

2.7.2 Domains

9. Information use and disclosure policy

- PHI should not be used for marketing purposes
- Hospital buys mailing lists from outside firms instead of using hospital's patient information
- Aggregative, de-identified data is used for feasibility studies. This information is used internally only & never to contact or solicit patients.
- Would allow mailings to patients for educational purposes only. Must be careful not to be too loose with the "educational" designation

2.7.3 Critical Observations

The two scenarios reveal that most stakeholders agree that the marketing use of their own protected health information without authorization from patients is simply unacceptable. One stakeholder used a third party marketing firm to obtain marketing data, despite the fact that they had the data, were uncomfortable using that in house data for marketing purposes.

2.8. 2.8. Public Health/Bioterrorism (Scenario 13)

2.8.1 Stakeholders

Stakeholders for this scenario included: State public health agency, local public health, hospitals and professional associations and societies.

2.8.2 Domains

1. User and entity authentication

- Access to systems are controlled through the use of user ids and passwords.

- In Michigan, Homeland Security is managed by the State Police. In this situation, the State Police would be invited to participate in the process.

4. Information transmission security or exchange protocols

- MDCH Bioterrorism and State Lab would contact the CDC, EPA & OPHP (phone call) and provide complete results.

- The Michigan Disease Surveillance System (MDSS) is double fire walled.

7. Administrative or physical security safeguards

- In case of a Public Health Emergency, such as a bioterrorism event, Public Health concerns trump HIPAA.

- Release of PHI in Public Health Emergency -- Public Health officials are given full access to PHI.

- Members from across MDCH and the Governor's Cabinet convene in a secure location and the event is managed from that location.

- Once the ICS is formed, information is readily shared among federal, state and county authorities based on strict hierarchical procedures.

- Activate Community Health Emergency Coordination Center (CHECC). CHECC convenes in a lockdown facility that has keycard access only. Security guards are posted at only entrance

- Use Michigan Emergency Medical Systems (MEMS) to track incident and notify medical personnel.

9. Information use and disclosure policy

- Epidemiology would provide case management and would track individual cases.

- Governor issues a state of emergency.

- Messages to the public and all outside entities are coordinated among federal, state and local entities.

- All lab results are sent not only to the ordering physician, but also to the State Lab

- If initial lab results indicate a threat, State Lab retests sample to confirm results

- Once confirmed positive, results are entered, tracked and disclosed to federal & state authorities via the Michigan Disease Surveillance System

- Generally age and gender only are released to the press

- Relevant Medical providers are notified of the situation via the HAN.
- an 800 number is set up for interested parties that includes de-identified information about the situation
- The State PR department handles press inquiries and typically only discloses age, gender and county information.
- All potentially affected households would receive an automated response regarding the situation that includes limited clinical information. The call would include instructions and next steps.

2.8.3 Critical Observations

No barriers to information sharing were noted, in fact, the universal response was bioterrorism and public health emergencies trump HIPAA. However, all participants noted that great pains were taken to insure that messages to the public were accurate, non-panic inducing and contained limited information regarding the affected.

2.9. Employee Health (Scenario 14)

2.9.1 Stakeholders

Stakeholders for this scenario included: Employers and Hospitals
.

2.9.2 Domains

1. User and entity authentication

- Provider electronically signs document.
- Access to systems are controlled through the use of user ids and passwords.
- Policy requires a "wet" signature on return to work form.2

4. Information transmission security or exchange protocols

- Access from one entity to another is provided via a secure connection or VPN
- Patient hand carries, provider faxes or mails PHI.
- PHI is encrypted prior to transmission. The encryption key is sent separately.

7. Administrative or physical security safeguards

- Employee forms that include confidential information are kept in a secure location and are locked.
- Employee data that includes confidential information is kept on a segregated, secure network drive.
- Any additional information the employee needs will be provided through the Follow up Nurse.

9. Information use and disclosure policy

- Dept of Labor form, which includes PHI is completed by physician and is submitted to employer in order to return to work in accordance with FMLA requirements.
- Return to work form was developed jointly between employer & union. Includes 7 data elements. Required after 5 days out due to illness or infirmary.

2.9.3 Critical Observations

One of the more surprising findings from this scenario is the requirement for a "wet" signature. The two reasons given for this requirement:

- It is a "high-touch" activity that provides the employee with a sense of control, and
- The company is so large that tracking who reports to whom is not a consistent exercise. Human resources would not be able to reliably route personnel messages to the current supervisor.

2.10. Public Health (Scenarios 15–17)

2.10.1 Stakeholders

Stakeholders for this scenario included: State public health agency, local public health, hospitals, state police, rhios and professional associations and societies

2.10.2 Domains

1. User and entity authentication

- Newborn blood spot cards are bar-coded for tracking of patient id.
- Access to systems are controlled through the use of user ids and passwords.

2. Information authorization and access controls

- Patient signs an Authorization or release of data authorization language is included in the NPP that the patient signs.
- User IDs are terminated when an employee quits and all user ids are reviewed on a regular basis to determine if they should be still active.
- Every three years, a provider's license is verified. If the provider does not have a valid license, access is terminated

3. Patient and provider identification

- A central database of credential providers is maintained. Facilities, provider groups and payers all agree to the base standards and share this information rather than credentialing independently. Providers are re-credentialed every 3 years & sanctions are monitored on a continual basis. Virtually all providers are included in every facility roster as a result.
- Doctors can search by Last Name & DOB with First Name and address optional. Duplicate entries are listed & doctor can select from list.
- Patient information is deleted when duplicate data is found.
- Newborn blood spot cards are bar-coded for tracking of patient id.
- Doctors can search by Last Name & DOB with First Name and address optional. Duplicate entries are listed & doctor can select from list

4. Information transmission security or exchange protocols

- Access from one entity to another is provided via a secure connection or VPN
- Patient hand carries, provider faxes or mails PHI.
- Provider makes copies of pertinent parts of medical records and Mail or fax to trading partner
- PHI is encrypted prior to transmission. The encryption key is sent separately.
- Confirm that recipient actually received the transmitted PHI
- The information is entered into the MDSS & is coded so only the code is included in emails.

- Birth Centers enter newborn's vital information into the State's public health portal via a secure connection

- Transmission to a monitored fax in a locked location

- The information is entered into the MDSS & is coded so only the code is included in emails

5. Information protection (against improper modification)

- Provide read-only access to ePHI

7. Administrative or physical security safeguards

- Information is zipped, encrypted & password protected & emailed. The password and encryption key is emailed separately, or provided via a phone call.

- MCIR has a complete disaster recovery plan & can be operational within 24 hours of most disasters.

- In case of a Public Health Emergency, such as a bioterrorism event, Public Health concerns trump HIPAA. Public Health officials are given full access to PHI.

8. State law restrictions

- Patient signs a separate Authorization to release MH, SA or HIV/AIDS related clinical data.

9. Information use and disclosure policy

- Release patient information to a family member is only allowed after the proper authorization has been signed by the patient granting that family member authorization.

- All newborns are tested for 22 genetic factors. All birthing facilities send the blood spots and lab results to the state lab. (Public health mandate.)

- Results of newborn screening, if positive are reported to the hospital and primary care physician. Results are faxed.

- MDCH Follow-up Group establishes course of treatment for affected newborns and monitors their progress.

- Lead screening results have been added to MCIR.

- State public health authority would call the CDC, since multiple states are involved. Full PHI would be shared with the CDC. The CDC would coordinate the full response.

- Generally age and gender only are released to the press.
- All lab results are sent not only to the ordering physician, but also to the State Lab for disease surveillance.
- If the patient is under court-ordered treatment, they have "failed to comply"/broken the law by leaving and the state police would be notified.
- CDC coordinates sharing of PHI between states and the transportation company.

2.10.3 Critical Observations

The only barrier noted is a state requirement to obtain a separate release of information for substance abuse data.

2.11. State Government Oversight (Scenario 18)

2.11.1 Stakeholders

Stakeholders for this scenario included: State public health agency and local public health.

2.11.2 Domains

1. User and entity authentication

- As part of issuing user ids and passwords, a provider's license is verified
- Providers are required to sign a user agreement in order to gain access to the system
- User ids are reviewed and monitored annually to ensure employees that access the system are still employed at the practice.
- The system supports role based access

2. Information authorization and access controls

- Users are required to sign a confidentiality agreement

3. Patient and provider identification

- Patients are identified by first name, last name and DOB. Additionally, address information is provided to distinguish potential duplicate.

- An automated process identifies potential duplicates that are then reviewed by MCIR staff. If the multiple entries are considered duplicates, a process merges the records into one.

4. Information transmission security or exchange protocols

- Access from one entity to another is provided via a secure connection or VPN

6. Information audits that record and monitor activity

- All user activity is logged and audit logs are reviewed on a regular basis. Penalty for improper access, use or disclosure includes terminated access for life, termination of employment or suspension.

7. Administrative or physical security safeguards

- CDC reviews and confidentiality agreement used by Public Health organization every 3 years

- MCIR has a complete disaster recovery plan & can be operational within 24 hours of most disasters.

8. State law restrictions

- State mandates that immunization data for all children under the age of 20 (from 1-1-94 to present) be entered into database. (Scope has recently been expanded to include adults and children.) MCIR has the authority of state legislative mandate as a public health initiative.

9. Information use and disclosure policy

- Doctors can access a child's immunization information in MCIR without obtaining parent's consent, since it is considered public health information.

- Patients or parents have the option to opt-out of tracking immunizations, etc. in MCIR. The default action is inclusion

- MCIR supports complete role-based access

2.11.3 Critical Observations

For this scenario, the universal response was "We would use MCIR." No one in Michigan seemed to want to consider any other approach.

The Michigan Care Improvement Registry (MCIR) was formed by:

- Sec. 333.5111 (1) b – Requirements for reporting communicable and serious communicable diseases R 325.173 – Administrative rules detailing the reporting of communicable and serious communicable diseases

- Sec. 33.9207 – Establishment of the Michigan Childhood Immunization Registry

- R.325.163 – Administrative rules requiring the reporting of immunizations administered to children to the Department of Community Health.

MCIR was created as a statewide public health initiative. At the time of its formation ten years ago, Michigan was dead last in childhood immunizations, (50^{th} out of 50 states.) The system provides a comprehensive immunization tracking for every child who lives in Michigan. Through widespread use and adoption of the system, Michigan is now 9th in the nation in childhood immunizations and rising in the ranks.

The many advantages of MCIR include:

- Doctors have the ability to look up a child's complete immunization record in a very short time period, without obtaining release of records or contact with other physicians or clinics.

- Reminders of overdue immunizations are sent directly to the doctor's office and letters are sent to parents.

MCIR is considered a "Best of Breed" public health initiative, and has been expanded to include adult immunizations (e.g. tetanus) in 2006.

3. Summary of Critical Observations and Key Issues

There were many key barriers and other issues of note collected during the process. Getting the healthcare community to share data in electronic form is clearly a complicated and multifaceted task. Identifying the privacy and security barriers is a beneficial starting point. However it should be noted that a plethora of issues exist, and they are not relegated to those of a technical nature.

Entities within the healthcare industry have a variety of functions and competing concerns. One of the major issues repeated throughout the interim assessment stage was the barrier relating to the creation of trust between those entities needing and wanting to share health information.

Generally other issues involved methods of securing user authorizations for those providers who were not credentialed at a particular entity. While credentialing prior to allowing access is a goal of many of the stakeholders, the overriding barrier with credentialing is the lack of timeliness.

Another critical barrier in Michigan revolves around emerging RHIOS. These newly forming entities are in need of consistent federal and state guidance. Because of the technology and structure of RHIOS is, in many cases ground breaking, standardization across the board will prove to be a key to their success. Particularly noted throughout the assessment period were conservative interpretations of HIPAA. The divergent views of how treatment, payment and healthcare operations are defined is a barrier to interoperability.

Non-healthcare entities approach interoperability in a different manner those involved in healthcare. There is a dramatic difference in how law enforcement officials handle things and how medical personnel handle similar situations.

Marketing and other non-clinical uses of health data received similar responses across the board. Providers from all fields were opposed to most non-clinical uses of healthcare data. Physicians were vocal in their opposition to using healthcare data for quality measurement.

The Michigan Care Improvement Registry (MCIR) is an excellent example of functioning health information exchange. Created to report communicable and serious communicable diseases, MCIR's success has propelled Michigan from being ranked last as a provider of childhood immunizations, to being 9th in the nation.

MCIR was created as a statewide public health initiative. At the time of its formation ten years ago, Michigan was dead last in childhood immunizations, (50th out of 50 states.) The system provides a comprehensive immunization tracking for every child who lives in Michigan. Through widespread use and adoption of the system, Michigan is now 9th in the nation in childhood immunizations and rising in the ranks.

Finally, a barrier in Michigan and perhaps in all the states, is the state-level requirement for enhanced protection of sensitive health information. In Michigan, as in many other states there are three categories of health information that require additional consent before being released. Those include HIV/AIDS data (Confidentiality of HIV or AIDS Test Results MCL 333.5131) , mental health records (Confidentiality of Mental Health Records MCL 330.1748) and substance abuse (Confidentiality of Substance Abuse Records MCL 333.6521).

4. Appendices